REMARKS

Claims 1-9, 12, 13 and 15-32 are pending, claims 1-9, 12, 13 and 15-23 are allowed and claims 24-32 are rejected.

A.   **Claims 24, 25 and 37-30 were rejected under 35 U.S.C. §103(a), as rendered obvious and unpatentable, over Fitzpatrick (US 5,420,936) in view of O'Connor (US 5,838,306) and Lane (US 5,623,552).** The Applicant respectfully traverses this rejection for the following reason(s).

Claims 24 and 25 calls for *a kernel of an operating system of the information device.*

Claim 24 requires that *the kernel determines whether the fingerprint data base has been established in the information device, recognizes that the external device and the information device have been activated and performs a fingerprint registration routine when it is determined that the fingerprint data base has not been established;* and

claim 25 requires that *the kernel determines whether the fingerprint data base has been established in the information device, recognizes that the external device and the information device have been activated and performs a fingerprint registration routine when it is determined that the fingerprint data base has not been established.*

The Examiner acknowledges that Fitzpatrick fails to teach the foregoing features. Here the Examiner relies on O'Connor and Lane, suggesting that one of ordinary skill in the art would have been motivated to modify Fitzpatrick's kernel to include the routine of O'Connor, and that it would

have been obvious to modify step 505 in O'Connor in view of Lane.

O'Connor fails to suggest modifying Fitzpatrick's kernel, and in fact, appears to teach away from such a modification. Teaching away from the invention is an important indication of non-obviousness. *See, e.g. Bausch & Lomb, Inc. v. Barnes-Hind/Hydrocurve, Inc. Inc.,* 796 F.2d 443, 230 USPQ 416 (Fed. Cir. 1986).

O'Connor's routine is performed by the BIOS. As is well known in the art, a kernel is a part of an operating system, and a BIOS is a program a personal computer's microprocessor uses to get the computer system started after you turn it on to **boot** the computer, and also manages data flow between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, mouse, and printer.

The BIOS is a separate entity from the computer's operating system, such that it is an integral part of a computer, but the operating system may be installed/replaced anytime after the computer is manufactured.

O'Connor teaches that the security feature is encoded into the Basic Input Output System (BIOS) so that the security function cannot be defeated by loading from a floppy disk when the computer is initiated or "booted". Col. 3, lines 38-41.

If the security feature of O'Connor were part of the kernel of the operating system, then it could be defeated as taught by O'Connor.

Lane fails to suggest modifying O'Connor's use of the BIOS to ensure proper security.

In paragraph 3 of the final rejection, the Examiner argues that O'Connor's teaching that the

security feature is encoded into the is an example only, and not meant to limit the use of the security feature.

The Examiner notes that O'Connor also discloses that the use of the security feature could be implemented by simply switching out the user's current mouse with a mouse capable of capturing fingerprints without having to make modifications to the BIOS, referring us to col. 3, lines 31-38, which state:

> Moreover, it is also anticipated that, in addition to its use in new systems, the device of the present invention may also be designed to include the associated electronics within the mouse itself to enable users to directly swap out the present invention with the mouse they are currently using, and receive the added functionality and features of the present invention.

Actually, O'Connor does not disclose that the use of the security feature could be implemented by simply switching out the user's current mouse with a mouse capable of capturing fingerprints, as suggested by the Examiner. In col. 3, lines 29-31 O'Connor discloses:

> The invention is designed to be used as a replacement for a typical PC mouse and will function as a standard mouse in all respects under normal use.

O'Connor does not suggest that the invention can be utilized by simply switching out the user's current mouse.

O'Connor describes the security mouse with respect to Fig. 1 and col. 3, line 42 through col. 4, line 15, and a block diagram of a signal processing scheme which may be implemented in practicing the present invention with respect to Fig. 2, in col. 4, lines 16-62.

Particularly, in col. 4, lines 58-62, O'Connor teaches:

-4-

It will be recognized that the signal processing scheme shown in FIG. 2 and described in detail above may be implemented by and within the mouse peripheral input device 101 (FIG. 1), the computer system (FIG. 4), or some combination of the two.

There is no suggestion in col. 4, lines 16-62 that the signal processing scheme be incorporated into a kernel of the operating system.

O'Connor goes on to give a detailed accounting of the invention which includes disclosure that Fig. 5 illustrates the method of the present invention as implemented **in a program** running on the computer system shown in FIG. 4; that Fig. 6 is **a BIOS routine** to validate a user entry 601 to the system; that Fig. 7 is a **Mouse Driver or Interrupt Service Routine** ; that Fig. 8 is a Check Fingerprint **Mouse Driver routine**; and that Fig. 9 is **an application security check routine** 901 which may be called from various places in secure applications.

There is no suggestion that the signal processing schemes of Figs. 5-9 be incorporated into a kernel of the operating system.

Instead, O'Connor suggests using some unspecified program, with regard to Fig 5, but notes in col. 1, lines 32-37, "a need for an apparatus and method to achieve high security protection of access to personal computers in an unobtrusive fashion **which will not require** additional desktop space or **re-programming of standard applications** for conventional use."

There are several standard operating systems currently in use, *i.e.,* Linux and Variants thereof; MacOS; MS-DOS; IBM OS/2 Warp; UNIX and Variants thereof; Windows CE; Windows 3.x; Windows 95; Windows 98; Windows 98 SE; Windows ME; Windows NT; Windows 2000; and

Windows XP, non of which incorporate a kernel that determines whether the fingerprint data base has been established in the information device, recognizes that the external device and the information device have been activated and performs a fingerprint registration routine when it is determined that the fingerprint data base has not been established.

Accordingly, O'Connor fails to suggest modifying Fitzpatrick's kernel, and the unspecified program of Fig. 5 appears to be a program specific to the mouse and not part of a standard operating system.

With regard to Figs. 7 and 8, O'Connor suggests utilizing a mouse driver, or subroutine (interrupt service routine) thereof. As is well known in the art, when purchasing a non-typical mouse to replace a typical mouse, a new mouse driver is required. The new mouse driver is clearly not a part of the system's standard operating system.

And with regard to Fig. 9 it is not clear whether the application security check routine is part of some secure application of a program like that of Fig. 5.

O'Connor makes no mention at all of an "operating system."

Deficiencies in the factual basis cannot be supplied by resorting to speculation or unsupported generalities. *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967) and *In re Freed*, 425 F.2d 785, 165 USPQ 570 (CCPA 1970).

Accordingly, one of ordinary skill in the art would not have been motivated by O'Connor to modify a kernel in Fitzpatrick's operating system.

Therefore, the rejection is deemed to be in error and should be withdrawn.

B. **Claims 26, 31 and 32 were rejected under 35 U.S.C. §103(a), as rendered obvious and unpatentable, over Fitzpatrick (US 5,420,936) in view of Postlewaite (US 5,854,891) in view of O'Connor (US 5,838,306) and Lane (US 5,623,552).** The Applicant respectfully traverses this rejection for the following reason(s).

Claim 26 also requires that *the kernel determines whether the fingerprint data base has been established in the information device, recognizes that the external device and the information device have been activated and performs a fingerprint registration routine when it is determined that the fingerprint data base has not been established.*

The Examiner acknowledges that Fitzpatrick fails to teach the foregoing features. Here the Examiner relies on O'Connor and Lane, suggesting that one of ordinary skill in the art would have been motivated to modify Fitzpatrick's kernel to include the routine of O'Connor, and that it would have been obvious to modify step 505 in O'Connor in view of Lane.

O'Connor fails to suggest modifying Fitzpatrick's kernel, as argued above with respect to claims 24 and 25.

Claim 26 differs from claims 24 and 25 in that it calls for *a kernel of an operating system of the information device permitting access to electronic commerce through the information device*

when the fingerprint verifying device determines that the transmitted fingerprint data match the registered fingerprint data. The Examiner has applied Postlewaite in this regard.

The Examiner suggests Postlewaite's teaching that:

> As smart cards supplant conventional magnetic strip enabling cards, new needs for expanded abilities in one card and for security arise. New abilities or functions include ability to communicate with different computers and also to be compatible with different computer operating software. This versatility is lacking in magnetic strip cards. However, as abilities increase, so does the potential for abuse of electronic transactions due to unauthorized access to computer programs which control bank and other financial accounts, and other sensitive matters (col. 1, lines 38-48);

"it would have been obvious to one of ordinary skill in the art to modify Fitzpatrick to store programs in nonvolatile storage (88) that are related to electronic commerce." Note that nonvolatile storage 88 in Fitzpatrick is separate and distinct for operating system 84, as shown in Fig. 4.

The Examiner fails to provide a *prima facie* basis of obviousness with respect to the claimed feature requiring *an operating system of the information device permitting access to electronic commerce through the information device.* Note that Postlewaite, like Fitzpatrick, makes no mention at all of *an operating system of the information device permitting access to electronic commerce through the information device.*

Therefore, the rejection is deemed to be in error and should be withdrawn.

The examiner is respectfully requested to reconsider the application, withdraw the objections and/or rejections and pass the application to issue in view of the above amendments and/or remarks.

Should a Petition for extension of time be required with the filing of this Amendment, the Commissioner is kindly requested to treat this paragraph as such a request and is authorized to charge Deposit Account No. 02-4943 of Applicant's undersigned attorney in the amount of the incurred fee if, **and only if**, a petition for extension of time be required **and** a check of the requisite amount is not enclosed.

Respectfully submitted,

Robert E. Bushnell,
Attorney for the Applicant
Registration No.: 27,774

1522 "K" Street N.W.,
Suite 300
Washington, D.C. 20005
(202) 408-9040

Folio: P56173
Date: 10/26/06
I.D.: REB/MDP